Acceptable Use Policy

Effective Date: September 29, 2025
Last Updated: September 29, 2025

This Acceptable Use Policy (“AUP”) is incorporated by reference into the Infinity Generation End User License Agreement.

Infinity Generation may update this Acceptable Use Policy from time to time in accordance with Section 14(c) of the End User License Agreement.

1. Overview

This Acceptable Use Policy ("AUP") governs the use of Infinity Generation software, editor tools, and any associated plugin marketplace or distribution services ("Platform", "Software", "we", "us", or "our") and applies to all users, developers, and contributors ("Users", "you", or "your") who use our procedural generation platform, develop plugins, or distribute content through our ecosystem. By using the Platform or distributing plugins through our marketplace/repository, you agree to comply with this AUP.

2. Scope

This policy applies to:

- Use of the Platform software and editor tools
- Development and distribution of plugins through our official marketplace, repository, or distribution channels
- Sharing of procedural generation assets, templates, and content
- Participation in our community forums, if applicable
- Use of our plugin development SDKs and APIs

3. Prohibited Plugin Development and Distribution

You agree NOT to create, distribute, or knowingly enable plugins that:

3.1 Malicious Software

- Contain viruses, worms, trojan horses, ransomware, spyware, keyloggers, or other malicious code

- Intentionally damage, disable, or impair user systems or data
- Create backdoors or unauthorized access mechanisms
- Hijack system resources for unauthorized purposes (e.g., cryptocurrency mining)
- Modify or delete user files without explicit user consent and clear disclosure

3.2 Security Exploits

- Exploit vulnerabilities in the Platform, operating systems, or other software
- Bypass, disable, or circumvent security features or license protections
- Facilitate unauthorized access to restricted content or features
- Include rootkits or code designed to hide malicious activity
- Compromise system integrity or stability
- Include proxy servers or other network redirection mechanisms
- Automatically redirect users to external websites or services without explicit user action
- Handle sensitive authentication information in an insecure manner

3.3 Privacy Violations

- Collect or transmit user data without clear disclosure and consent
- Include hidden tracking, analytics, or telemetry not disclosed in plugin documentation
- Harvest personal information, credentials, or authentication tokens
- Violate applicable privacy laws and regulations
- Implement covert surveillance or monitoring capabilities

3.4 Deceptive Practices

- Misrepresent plugin functionality or purpose
- Include hidden or undocumented features
- Impersonate official Platform plugins or other legitimate software
- Use misleading names, descriptions, or metadata
- Bundle unwanted or undisclosed additional software

3.5 Intellectual Property Violations

- Infringe upon copyrights, trademarks, patents, or trade secrets
- Include pirated content or license keys
- Circumvent digital rights management (DRM) or copy protection
- Redistribute proprietary code without authorization
- Violate open source licenses when using third-party code

3.6 Illegal Content or Activities

- Facilitate or enable illegal activities in any jurisdiction
- Generate content that violates applicable laws
- Include content that exploits minors
- Produce outputs that could be used for fraud, harassment, or other harmful purposes
- Create tools primarily designed for illegal purposes
- Promote or encourage drug trafficking, money laundering, or terrorist activities
- Facilitate gambling operations where prohibited by law
- Enable circumvention of export control regulations

3.7 Code Quality and Stability

- Contain code that throws unhandled errors or warnings during normal operation
- Include memory leaks or resource management issues that degrade system performance
- Use deprecated or unsafe functions without proper safeguards
- Contain race conditions or threading issues that cause instability
- Include obfuscated code solely to hide malicious functionality (legitimate IP protection through obfuscation is permitted with disclosure)

3.8 AI-Generated Content

- Use AI-generated code or content without proper validation and testing
- Include AI-generated content that infringes on third-party intellectual property

- Distribute AI-generated content that contains anatomical errors, technical flaws, or safety issues
- Fail to disclose the use of AI generation tools where such content impacts functionality or safety

4. Plugin Development Standards

All plugins distributed through our official channels must:

4.1 Technical Requirements

- Be compatible with supported Platform versions as specified
- Include accurate version information and dependency declarations
- Handle errors gracefully without causing system instability
- Respect system resources and user-defined performance settings
- Properly clean up resources upon uninstallation

4.2 Documentation and Disclosure

- Provide clear, accurate descriptions of functionality
- Disclose all system permissions required
- Document any network communications or external connections
- List all third-party dependencies and their licenses
- Include uninstallation instructions if applicable

4.3 User Consent and Control

- Request user permission for any file system operations outside designated plugin directories
- Allow users to disable or configure any data collection
- Respect user preferences and system settings
- Provide clear opt-in/opt-out mechanisms for optional features
- Not execute any code that automatically runs on system startup without explicit user consent

- Not modify system registry or configuration files without clear disclosure and consent

4.4 Third-Party Components

- Properly attribute all third-party code, libraries, and assets used
- Ensure all dependencies are compatible with intended use cases
- Include required license files for any third-party components
- Not include dependencies with restrictive licenses (GPL, LGPL) that would affect user projects
- Clearly document all external dependencies and their versions

5. Content Guidelines

Procedural content, templates, and assets shared through the Platform should not:

- Include hate speech or discriminatory content
- Contain sexually explicit material in non-age-appropriate contexts
- Promote violence or self-harm
- Infringe on intellectual property rights
- Violate any applicable laws or regulations

6. Use of Platform Software

Users of the Platform software agree to:

- Use the software only for lawful purposes
- Not reverse engineer, decompile, or disassemble the software except as permitted by law
- Not remove or alter any proprietary notices
- Comply with all applicable export control laws
- Not use the software to develop competing products without authorization

7. AI Training and Machine Learning Use

7.1 License Requirements for ML Training

- Users who utilize any data generated by the Platform to train, fine-tune, or otherwise develop machine learning models, neural networks, or AI systems MUST have an active license tier that explicitly permits machine learning training use
- This requirement applies regardless of whether the training is for commercial or non-commercial purposes
- Standard licenses do not include ML training rights unless explicitly stated

7.2 Usage Tracking and Monitoring

- Users engaging in ML training with Platform-generated data must enable and maintain usage telemetry features
- Disabling, blocking, or circumventing usage tracking while using generated data for ML training constitutes a violation of this AUP
- Usage tracking monitors software usage patterns only and does not collect or transmit generated content (users retain full ownership of their generated data)

7.3 Compliance and Enforcement

- Violation of ML training license requirements will result in immediate license termination
- Users found in violation of ML training terms acknowledge that such violation constitutes willful infringement and may result in enhanced damages
- We reserve the right to audit usage patterns to ensure compliance with ML training license requirements
- Users must maintain records demonstrating compliance if using generated data for ML training

8. Reporting and Enforcement

8.1 Reporting Violations

If you discover a plugin that violates this AUP, especially those containing malicious code or security vulnerabilities, please report it immediately to contact@infinitygeneration.com. We support responsible disclosure and may offer bug bounties for qualifying security reports.

To report suspected violations of ML training license requirements or unauthorized AI training use, please contact [compliance email] with any available evidence.

8.2 Enforcement Actions

Violations of this AUP may result in:

- Removal of plugins from official distribution channels
- Revocation of developer access and publishing privileges
- Blacklisting of code signatures or developer certificates
- Public disclosure of malicious plugins to protect users
- Cooperation with law enforcement when appropriate
- Legal action to recover damages
- Immediate license termination without refund
- Forfeiture of any indemnification or limitation of liability protections under our Terms of Service
- In cases of ML training violations, pursuit of willful infringement remedies

8.3 Review Process

We may implement automated and manual review processes for plugins. However, users acknowledge that:

- Not all plugins may be reviewed before distribution
- Reviews may not detect all policy violations or security issues
- Users are ultimately responsible for evaluating plugins before installation

9. Disclaimer and Limitation of Liability

THE PLATFORM IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. We do not guarantee that all plugins are safe, functional, or compliant with this AUP. Users install and run plugins at their own risk. We strongly recommend:

- Only installing plugins from trusted developers
- Reviewing plugin source code when available
- Maintaining regular backups
- Using appropriate security software

9. Modifications to This Policy

We reserve the right to modify this AUP at any time. Significant changes will be communicated through the Platform software, our website, or developer channels. Continued use of the Platform or distribution of plugins after changes constitutes acceptance.

10. Developer Certification

By submitting plugins for distribution through our official channels, developers certify that:

- They have the right to distribute the plugin and its contents
- The plugin complies with this AUP
- All disclosures about the plugin's functionality are accurate and complete
- They will promptly address security vulnerabilities when discovered

11. Contact Information

General Inquiries: contact@infinitygeneration.com
Security Issues: contact@infinitygeneration.com
Plugin Review/Compliance: contact@infinitygeneration.com
Address: 522 W Riverside Ave
Ste 5433
Spokane, WA 99201

By using the Platform software or distributing plugins through our ecosystem, you acknowledge that you have read, understood, and agree to be bound by this Acceptable Use Policy.